

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-004249
 (43)Date of publication of application : 06.01.1999

(51)Int.CI. H04L 12/46
 H04L 12/28
 H04L 9/36
 H04L 12/56

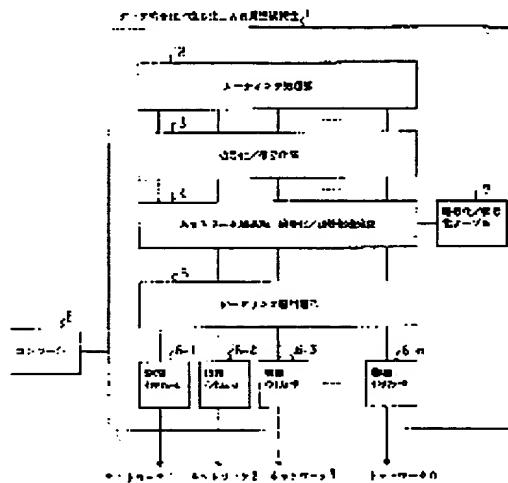
(21)Application number : 09-171110 (71)Applicant : NEC CORP
 (22)Date of filing : 12.06.1997 (72)Inventor : MATSUKAWA YOSHIKI

(54) CONNECTION DEVICE BETWEEN DATA CIPHERING/DECODING LAN

(57)Abstract:

PROBLEM TO BE SOLVED: To provide inter-LAN connection device ciphering and decoding the data part of a network layer with the address of the network layer in the packet of LAN.

SOLUTION: The connection device 1 is provided with a ciphering/decoding table 7 and a network layer processing/ciphering/decoding decision part 4 comparing the addresses in the header of the network layer and deciding whether the data part of the network layer is to be ciphered/decoded or not, and a ciphering/decoding part 3 executing ciphering/decoding by adjusting it to a content decided in the network layer processing/ciphering/decoding decision part 4.



LEGAL STATUS

[Date of request for examination] 29.07.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3259660

[Date of registration] 14.12.2001

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-4249

(43)公開日 平成11年(1999)1月6日

(51) Int.Cl.⁶
 H 04 L 12/46
 12/28
 9/36
 12/56

識別記号

F I
 H 04 L 11/00 310C
 9/00 685
 11/20 102D

審査請求 有 請求項の数6 FD (全9頁)

(21)出願番号 特願平9-171110
 (22)出願日 平成9年(1997)6月12日

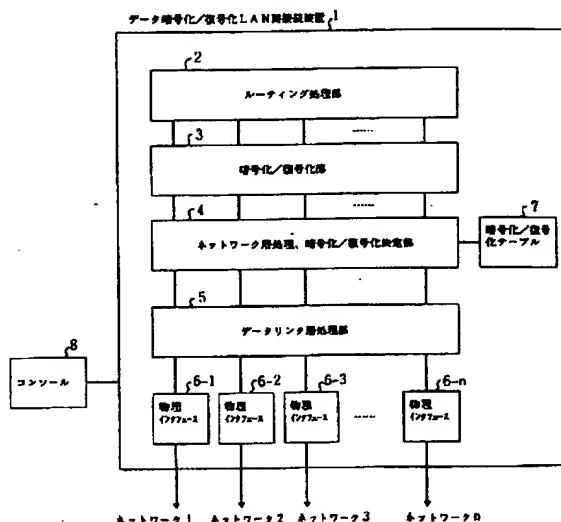
(71)出願人 000004237
 日本電気株式会社
 東京都港区芝五丁目7番1号
 (72)発明者 松川良樹
 東京都港区芝五丁目7番1号 日本電気株
 式会社内
 (74)代理人 弁理士 福山正博

(54)【発明の名称】 データ暗号化/復号化LAN間接続装置

(57)【要約】

【課題】 LANのパケットにおけるネットワーク層のアドレスによって、ネットワーク層のデータ部を暗号化、復号化するLAN間接続装置を提供する。

【解決手段】 暗号化/復号化テーブル7とネットワーク層のヘッダにあるアドレスとを比較し、ネットワーク層のデータ部を暗号化/復号化するか又はしないかを決定するネットワーク層処理・暗号化/復号化決定部4を設けると共に、ネットワーク層処理・暗号化/復号化決定部4で決定した内容に合わせて暗号化/復号化を行なう暗号化/復号化部3を備えるようにした。



1

【特許請求の範囲】

【請求項 1】 LANパケットをネットワーク層で中継するLAN間接続装置において、ネットワーク単位、LAN端末単位毎に暗号化または復号化を行なうために、LANのネットワーク層のアドレス、暗号化、復号化の有無を登録する暗号化／復号化テーブルと、

受信したLANパケットのネットワーク層のアドレスを監視し、前記テーブルを参照して暗号化／復号化の判定を行なう手段と、

この手段の判定に基づいて受信したLANパケットのネットワーク層のデータ部を暗号化／復号化を行なう手段と、を備えたことを特徴とするデータ暗号化／復号化LAN間接続装置。

【請求項 2】 LANパケットのネットワーク層のデータが暗号化済みまたは復号化済みであることを検出し、暗号化済みのものは前記テーブルで暗号化指定があつても暗号化せず、復号化済みのものは前記テーブルで復号化指定があつても復号化しないように二重処理を阻止する手段を備えたことを特徴とする請求項 1 に記載のデータ暗号化／復号化 LAN間接続装置。

【請求項 3】 ルーティングプロトコルを処理し、ルーティングテーブルを作成、受信したパケットのネットワーク層のヘッダにあるアドレスと前記ルーティングテーブルより、パケットを送信する物理インタフェースを決定するルーティング処理部と、、暗号化／復号化テーブルと、

送受信パケットのネットワーク層の誤り確認、ネットワーク層のヘッダ付替え、フラグメント処理などのネットワーク層の管理と、前記暗号化／復号化テーブルとネットワーク層のヘッダにあるアドレスとを比較し、ネットワーク層のデータ部を暗号化／復号化するか否かを決定するネットワーク層処理・暗号化／復号化決定部と、、前記ネットワーク層処理・暗号化／復号化決定部で決定した内容に合わせて暗号化／復号化を行なう暗号化／復号化部と、

送受信パケットのデータリンク層の誤り確認、フレームチェックシーケンスの生成、ヘッダの付替えなどを行なうデータリンク層処理部と、

それぞれネットワークに接続されており、LANパケットデータの送受信が行なわれる物理インタフェースと、LAN間接続装置に接続されており、ネットワークを管理するユーザーが、前記暗号化／復号化テーブルを設定するために用いられ、前記ルーティング処理部のルーティングテーブルの設定を行なうコンソールと、を備えて成ることを特徴とするデータ暗号化／復号化 LAN間接続装置。

【請求項 4】 前記通常データと暗号化データとの区別は、暗号化時にネットワーク層データの先頭または分散して暗号化識別子を付加し、これを検出することにより

2

区別する請求項 3 に記載のデータ暗号化／復号化 LAN間接続装置。

【請求項 5】 暗号化済み、復号化済みであるか否かを検出し、暗号化されているデータについてさらに暗号化したり、また復号化されているデータについてさらに復号化する請求項 3 に記載のデータ暗号化／復号化 LAN間接続装置。

【請求項 6】 前記暗号化及び復号化済みであるにも拘らず、前記ネットワーク層処理・暗号化／復号化決定部で重複して暗号化／復号化の指示がなされても、暗号化／復号化を行なわない請求項 3 に記載のデータ暗号化／復号化 LAN間接続装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データ暗号化／復号化 LAN間接続装置に関し、特に LAN間を跨いで端末間で通信されるデータの暗号化／復号化を行なう手段の改良に関する。

【0002】

【従来の技術】 従来のこの種の LAN間接続装置として、物理インタフェース毎に暗号化／復号化機能を有し、これらの物理インタフェースにおいて、送受信する全てのパケットデータに対し暗号化／復号化を行なうようにしたものがある。たとえば特開平 7-193589 号公報には、物理インタフェース単位に暗号化回路を附加する技術が開示されている。

【0003】 また、従来のこの種の LAN間接続装置として、LAN端末間で特別な暗号化ソフトウェアを導入し、当該端末間で暗号化する方式のものがある。たとえば、特開平 2-4037 号公報には、ファイルサーバーとユーザーとの間でユーザ識別子をパケットに附加して暗号化する技術が開示されている。

【0004】 さらに従来のこの種の LAN間接続装置として、LAN間接続を行なわない暗号化サーバー、復号化サーバーを用意して、暗号化及び復号化を行なうようにしたものがある。たとえば特開平 7-170280 号公報には、暗号化サーバー及び復号化サーバーを用いて暗号通信、復号通信を行なうローカルエリアネットワーク方式が開示されている。

【0005】

【発明が解決しようとする課題】 上記した従来の LAN間接続装置には以下のようない下の解決すべき問題点がある。第 1 の問題点は、物理インタフェース毎に暗号化／復号化するものでは、ルーティングに用いられるアドレス部分まで暗号化されるため、途中に暗号化／復号化を行なわない LAN間接続装置を介在させることができない。また暗号化／復号化する必要の無い宛先のデータも暗号化／復号化されるため、データの送受信に余分な時間を要する。

【0006】 第 2 の問題点は、LAN端末間で特別な暗

50

号化ソフトウェアを導入するものでは、現在、一般に用いられている通信ソフトウェアの他に、暗号化／復号化ソフトウェアを付加するか、或いは別の通信ソフトウェアを導入する必要がある。

【0007】第3の問題点は、暗号化サーバー、復号化サーバーを用意し、暗号化を行なうものでは、端末からサーバーに暗号化要求とデータとを送信し、サーバーが暗号化後、サーバーからの暗号化データを端末が受信し、その後、端末が実際のデータ転送先に送信する手続きが発生し、同じ内容のデータが端末とサーバーとの間で二度送受信されるという不具合がある。またサーバーに負荷が集中するという問題もある。

【0008】本発明の目的は下記の効果を奏するデータ暗号化／復号化 LAN間接続装置を提供することにある。

【0009】

【課題を解決するための手段】前述の課題を解決するため、本発明による暗号化／復号化 LAN間接続装置は、LANパケットをネットワーク層で中継する LAN間接続装置において、ネットワーク単位、LAN端末単位毎に暗号化または復号化を行なうために、LANのネットワーク層のアドレス、暗号化、復号化の有無を登録する暗号化／復号化テーブルと、受信した LANパケットのネットワーク層のアドレスを監視し、前記テーブルを参照して暗号化／復号化の判定を行なう手段と、この手段の判定に基づいて受信した LANパケットのネットワーク層のデータ部を暗号化／復号化を行なう手段とを備えて構成される。

【0010】換言すれば、暗号化／復号化テーブルとネットワーク層のヘッダにあるアドレスとを比較し、ネットワーク層のデータ部を暗号化／復号化するか否かを決定するためのネットワーク層処理・暗号化／復号化決定部を設けると共に、上記ネットワーク層処理・暗号化／復号化決定部で決定した内容に合わせて暗号化／復号化を行なう暗号化／復号化部を設けた。

【0011】また、本発明による暗号化／復号化 LAN間接続装置は、上記に記載した装置であって、かつ LANパケットのネットワーク層のデータが暗号化済みまたは復号化済みであることを検出し、暗号化済みのものは前記テーブルで暗号化指定があっても暗号化せず、復号化済みのものは前記テーブルで復号化指定があっても復号化しないように二重処理を阻止する手段を備える。

【0012】更に、本発明の他の態様による暗号化／復号化 LAN間接続装置は、ルーティングプロトコルを処理し、ルーティングテーブルを作成、受信したパケットのネットワーク層のヘッダにあるアドレスと前記ルーティングテーブルより、パケットを送信する物理インタフェースを決定するルーティング処理部と、暗号化／復号化テーブルと、送受信パケットのネットワーク層の誤り確認、ネットワーク層のヘッダ付替え、フラグメント処

埋などのネットワーク層の管理と、前記暗号化／復号化テーブルとネットワーク層のヘッダにあるアドレスとを比較し、ネットワーク層のデータ部を暗号化／復号化するか否かを決定するネットワーク層処理・暗号化／復号化決定部と、前記ネットワーク層処理・暗号化／復号化決定部で決定した内容に合わせて暗号化／復号化を行なう暗号化／復号化部と、送受信パケットのデータリンク層の誤り確認、フレームチェックシーケンスの生成、ヘッダの付替えなどを行なうデータリンク層処理部と、それぞれネットワークに接続されており、LANパケットデータの送受信が行なわれる物理インタフェースと、LAN間接続装置に接続されており、ネットワークを管理するユーザーが、前記暗号化／復号化テーブルを設定するために用いられ、前記ルーティング処理部のルーティングテーブルの設定を行なうコンソールとを備えて成る。

【0013】ここで、前記通常データと暗号化データとの区別は、暗号化時にネットワーク層データの先頭または分散して暗号化識別子を付加し、これを検出することにより区別する。また、暗号化済み、復号化済みであるか否かを検出し、暗号化されているデータについてさらに暗号化したり、また復号化されているデータについてさらに復号化する。更には、前記暗号化及び復号化済みであるにも拘らず、前記ネットワーク層処理・暗号化／復号化決定部で重複して暗号化／復号化の指示がなされても、暗号化／復号化を行なわない。

【0014】

【発明の実施の形態】図1は本発明の第1実施形態に係る LAN間接続装置の構成を示すブロック図である。図1に示すように LAN間接続装置1は、ルーティング処理部2、暗号化／復号化部3、ネットワーク層処理・暗号化／復号化決定部4、データリンク層処理部5、物理インタフェース6-1ないし6-n、暗号化／復号化テーブル7等を備えている。

【0015】ルーティング処理部2は、ルーティングプロトコルを処理し、ルーティングテーブルを作成、受信したパケットのネットワーク層のヘッダにあるアドレスと上記ルーティングテーブルより、パケットを送信する物理インタフェースを決定する。

【0016】暗号化／復号化部3は、ネットワーク層処理・暗号化／復号化決定部4で決定した内容に合わせて暗号化／復号化を行なう。また暗号化済み、復号化済みであるか否かを検出し、暗号化されているデータについてさらに暗号化したり、また復号化されているデータについてさらに復号化したりしない様になっている。すなわち、暗号化及び復号化済みであるにも拘らず、ネットワーク層処理・暗号化／復号化決定部4で重複して暗号化／復号化の指示がなされても、暗号化／復号化を行なわない機能を有している。

【0017】通常データと暗号化データとの区別は、暗

号化時にネットワーク層データの先頭または分散して暗号化識別子を付加し、これを検出することにより区別する。

【0018】ネットワーク層処理・暗号化/復号化決定部4は、送受信パケットのネットワーク層の誤り確認、ネットワーク層のヘッダ付替え、フラグメント処理などのネットワーク層の管理と、暗号化/復号化テーブル7とネットワーク層のヘッダにあるアドレスとを比較し、ネットワーク層のデータ部を暗号化/復号化するか否かを決定する機能を有している。

【0019】データリンク層処理部5は、送受信パケットのデータリンク層の誤り確認、フレームチェックシーケンスの生成、ヘッダの付替えなどを行なう。

【0020】各物理インターフェース6-1ないし6-nは、それぞれネットワーク1からnに接続されており、これらの物理インターフェース6-1ないし6-nを通して、LANパケットデータの送受信が行なわれる。

【0021】コンソール8は、LAN間接続装置1に接続されており、ネットワークNWを管理するユーザーが、暗号化/復号化テーブル7を設定するために用いられる。またコンソール8は、ルーティング処理部2のルーティングテーブルの設定等、本実施形態におけるLAN間接続装置1のその他の設定を行なうためにも用いられる。

【0022】次に、図2を参照して暗号化/復号化テーブルのテーブル要素について説明する。図2は暗号化/復号化テーブルのテーブル要素9を示す図で、図示の如く、事前に送信先アドレスN1、送信先ネットワークマスクM1、送信元アドレスN2、送信元ネットワークマスクM2、暗号化/復号化の有無X1、などを設定しておく。テーブルの1ラインには、暗号化/復号化の有無X1の項目を除く全ての項目を設定する必要はない。設定されなかった項目は暗号化/復号化の決定に用いられない。ネットワークマスクM1及びM2は、暗号化/復号化で参照される送信先アドレスN1及び送信元アドレスN2の部位を決定するために用いられる。この組み合わせによって、暗号化及び復号化を決定するネットワーク及びLAN端末が指定される。

【0023】図3はLANのパケットフォーマット10を示す図である。図示の如くこのパケットフォーマット10は、データリンク層ヘッダ部11、ネットワーク層ヘッダ部12、ネットワーク層データ部13、データリンク層フレームチェックシーケンス部14から成る。ここで暗号化/復号化されるのはネットワーク層データ部13である。

【0024】図4は本実施形態のLAN間接続装置1のパケット処理の動作にかかるパケット処理フローを示す図である。処理ステップ15では、物理インターフェース6-1ないし6-nにおいてパケットの受信が行なわれる。処理ステップ16では、データリンクアドレスの確

認、フレームの誤り確認などデータリンク層の受信処理が行なわれる。

【0025】処理ステップ17では、ネットワーク層処理・暗号化/復号化決定部4においてネットワーク層の誤り確認、フラグメント処理などネットワーク層の処理が行なわれた後、暗号化/復号化テーブル7を参照し暗号化または復号化の是非が判定される。暗号化/復号化を行なうことが決定された場合には、暗号化/復号化部3に対して暗号化/復号化指示が行なわれ、処理ステップ18に移る。暗号化/復号化は行なわないと決定された場合には、ルーティング処理部2に対しルーティング要求が出され、処理ステップ20に移る。

【0026】処理ステップ18では、暗号化済み/復号化済みの判定が行なわれ、未暗号化/未復号化の場合には、暗号化/復号化したのち処理ステップ20に移る。暗号化/復号化済みである場合には、そのまま処理ステップ20に移る。

【0027】処理ステップ20では、受信パケットの宛先アドレスとネットワーク層のルーティングテーブルより物理インターフェース6-1ないし6-nのいずれにパケットを出力するかが決定され、処理ステップ21に移る。

【0028】処理ステップ21では、ヘッダの付替え、フラグメントの処理などのネットワーク層の処理が行なわれ、処理ステップ22に移る。

【0029】処理ステップ22では、データリンク層のフレームチェックシーケンスの生成、ヘッダの付替えなどデータリンク層の出力処理が行なわれる。そして処理ステップ23では処理ステップ20で決定した物理インターフェース6-1ないし6-nにパケットが出力される。

【0030】以上の動作により、通常データの暗号化または暗号化データの復号化とその後の中継または通常データが中継される。

【0031】図5は、本発明の第2実施形態に係る「複数の本発明装置を用いたLAN間接続ネットワーク」の構成例を示す図である。一つの装置(X)24にはネットワーク(A)26、ネットワーク(B)27、ネットワーク(C)28が接続されている。ネットワーク(A)26には端末(a)30が接続され、ネットワーク(B)27には別の装置(Y)25が接続されている。そして装置(Y)25にはネットワーク(D)29が接続され、更にその先に端末(d)31が接続されている。装置(X)24及び装置(Y)25には、暗号化/復号化テーブルが設定されている。

【0032】図6及び図7は、装置(X)24及び装置(Y)25において、ネットワーク(A)26及びネットワーク(D)29で暗号化/復号化通信を行なう場合のテーブル設定例を示す図である。

【0033】端末(a)30は、端末(d)31向けに

パケットを送信を行なうべく、装置 (X) 24 にデータを送る。

【0034】装置 (X) 24 は、図6に示す暗号化/復号化テーブルを参照し、ネットワーク (D) 29 向けであって、かつ暗号化すべきデータである事を判定して暗号化し、ルーティング処理した結果、ネットワーク (B) 27 に接続されている装置 (Y) 25 に暗号化パケットを送信する。

【0035】装置 (Y) 25 は、装置 (X) 24 からの暗号化データを受信後において、図7に示す暗号化/復号化テーブルを参照し、ネットワークアドレスより復号化すべきデータである事を判定して復号化し、ルーティング処理した結果、ネットワーク (D) 29 に接続されている端末 (d) 31 に復号化データを送信する。

【0036】端末 (d) 31 から端末 (a) 30 へのデータも同様に暗号化/復号化され、端末 (a) 30 では復号化された端末 (d) 31 のデータが受信される。

【0037】一方、端末 (a) 30 から装置 (X) 24 経由でネットワーク (D) 29 以外のネットワーク向けにパケットが送信された場合は、図6に示す装置 (X) 24 の暗号化/復号化テーブルには暗号化/復号化指示が設定されていないので、そのまま暗号化されずに送信される。

【0038】本実施形態において、装置 (X) 24 と装置 (Y) 25との間に暗号化/復号化機能を持たない LAN間接続装置を接続した場合、ネットワーク層のデータ部は暗号化されるが、データリンク層、ネットワーク層のヘッダは暗号化されていないので、問題なく上記と同様に端末 (a) 30 と端末 (d) 31 とで暗号化/復号化通信を行なうことができる。

【0039】また、装置 (X) 24 と装置 (Y) 25との間に、本発明装置が接続された場合、設定如何によつては暗号化が二度発生する可能性がある。例えば装置 (X) 24 と装置 (Y) 25との間に他の装置を追加し、追加した装置にネットワーク (D) 29 向けのパケット全てを暗号化するように設定した場合、ネットワーク (A) 26 からネットワーク (D) 29 向けに送信されたパケットは装置 (X) 24 で暗号化され、さらに追加された装置で、このネットワーク (D) 29 向けのパケットに対し暗号化指示が発生する。しかし暗号化/復号化部3において暗号化済み、復号化済みの検出を行なっているので、追加された装置内で暗号化が二度行なわれることはなく、装置 (Y) 25 に転送される。よって、この場合は上記の暗号化/復号化機能を持たない LAN間接続装置を接続した場合と同様、端末 (a) 30 と端末 (d) 31との間で暗号化/復号化通信を行なうことができる。

【0040】

【発明の効果】本発明によれば、ネットワーク層のデータ部のみを暗号化するように構成されているため、装置

以外のネットワーク層をルーティングする LAN間接続装置についてルーティングでき、ネットワーク層レベルで標準的なパケットを出力することができる。かくして、インターネットや既に敷設されている TCP/IP ネットワークなどにそのまま接続でき、必要なネットワーク、 LAN端末間通信に対して暗号化/復号化を行なうことができる。また、ネットワーク単位、 LAN端末単位毎に暗号化/復号化の設定ができるため、暗号化/復号化する必要のない宛先のデータについてまで暗号化/復号化されるのを回避することができる。更に、 LAN間接続装置の間で暗号化/復号化が行なわれるため、 LAN端末間で特別な暗号化ソフトウェアを導入したり、暗号化サーバー、復号化サーバー等を用意したりする必要がない。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係るデータ暗号化/復号化 LAN間接続装置の構成を示すブロック図である。

【図2】本発明の第1実施形態に係るデータ暗号化/復号化 LAN間接続装置のネットワーク層処理、暗号化/復号化決定部において、暗号化/復号化を決定するため用いられる暗号化/復号化テーブルのテーブル要素を示す図である。

【図3】本発明の第1実施形態に係るデータ暗号化/復号化 LAN間接続装置が扱う LANのパケットフォーマットを示す図である。

【図4】本発明の第1実施形態に係るデータ暗号化/復号化 LAN間接続装置における LANのパケット受信から送信までのパケット処理フローを示す図である。

【図5】本発明の第2実施形態に係る「複数のデータ暗号化/復号化 LAN間接続装置を用いた LAN間接続ネットワーク」の構成例を示す図である。

【図6】本発明の第2実施形態に係るデータ暗号化/復号化 LAN間接続装置で設定される装置 (X) の暗号化/復号化テーブルのパターン例を示す図である。

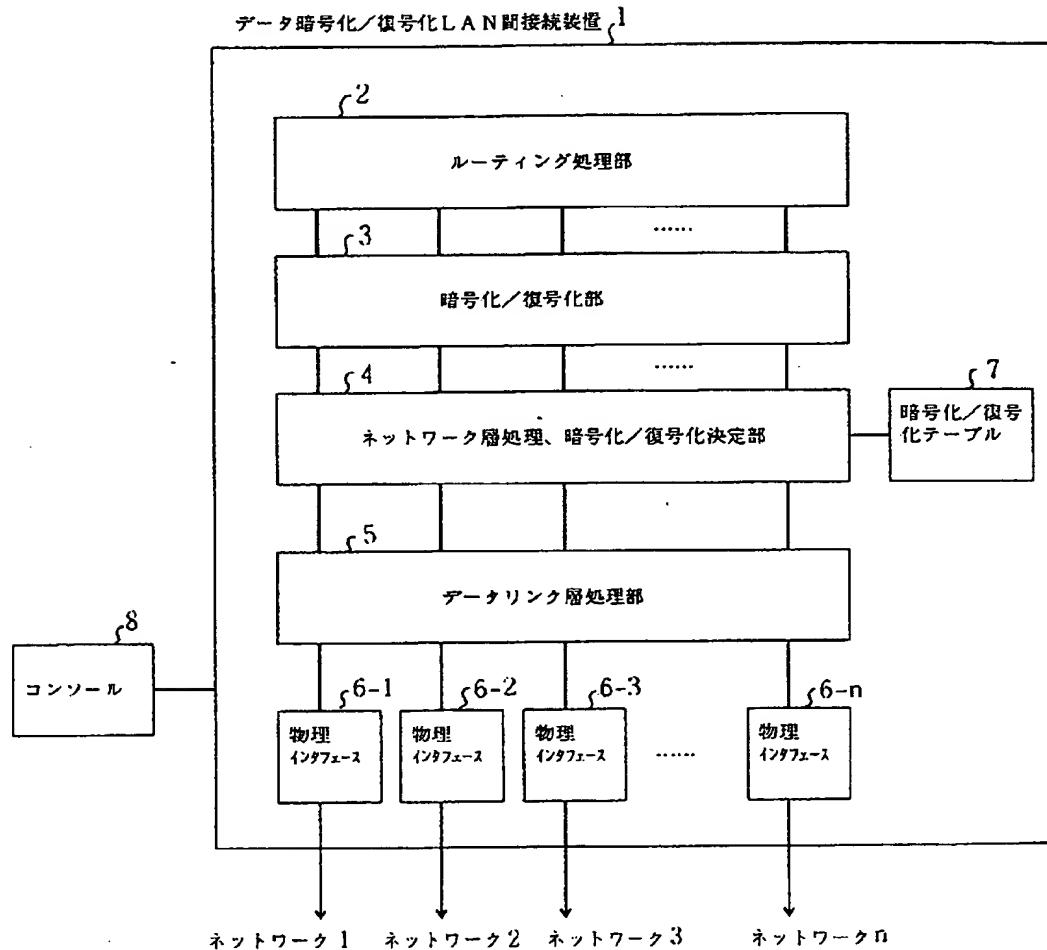
【図7】本発明の第1実施形態に係るデータ暗号化/復号化 LAN間接続装置で設定される装置 (Y) の暗号化/復号化テーブルのパターン例を示す図である。

【符号の説明】

1	データ暗号化/復号化 LAN間接続装置
2	ルーティング処理部
3	暗号化/復号化部
4	ネットワーク層処理・暗号化/復号化決定部
5	データリンク層処理部
6-1 ~ 6-n	物理インターフェース
7	暗号化/復号化テーブル
8	コンソール
9	暗号化/復号化テーブルのテーブル要素
10	LANパケットフォーマット
11	データリンク層ヘッダ部
12	ネットワーク層ヘッダ部

9	10
1 3 ネットワーク層データ部	* 2 9 ネットワーク (D)
1 4 データリンク層フレームチェックシーケンス部	3 0 端末 (a)
2 4 LAN間接続装置 (X)	3 1 端末 (d)
2 5 LAN間接続装置 (Y)	3 2 LAN間接続装置 (X) の暗号化／復号化テー ブル
2 6 ネットワーク (A)	3 3 LAN間接続装置 (Y) の暗号化／復号化テー ブル
2 7 ネットワーク (B)	
2 8 ネットワーク (C)	*

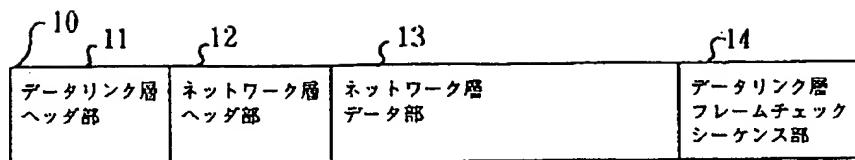
【図 1】



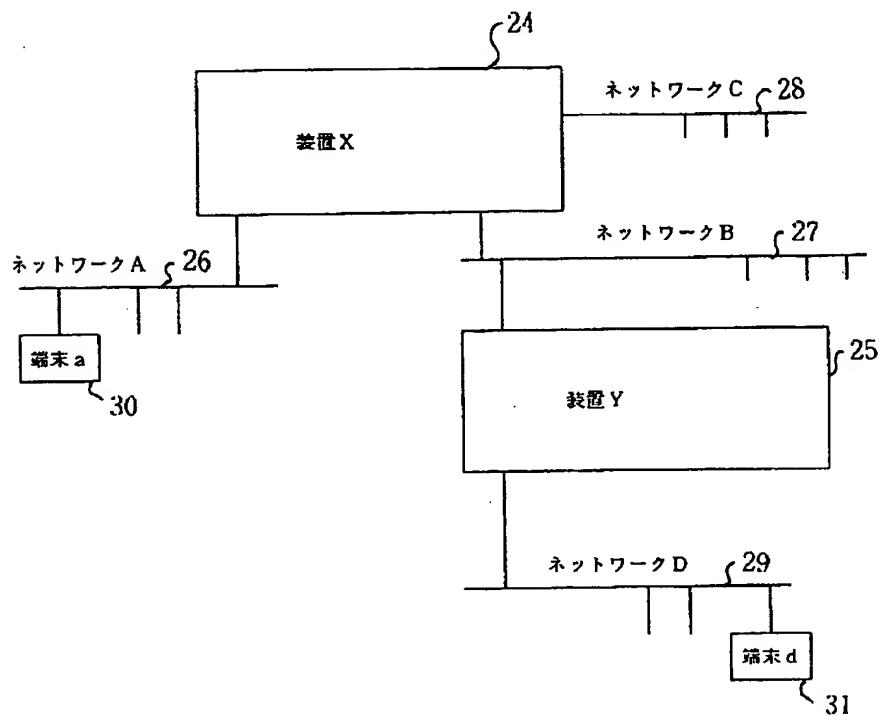
【図 2】

送信先アドレス	送信先ネットワークマスク	送信元アドレス	送信元ネットワークマスク	暗号化復号化種別
N 1	M 1	N 2	M 2	X 1

【図3】



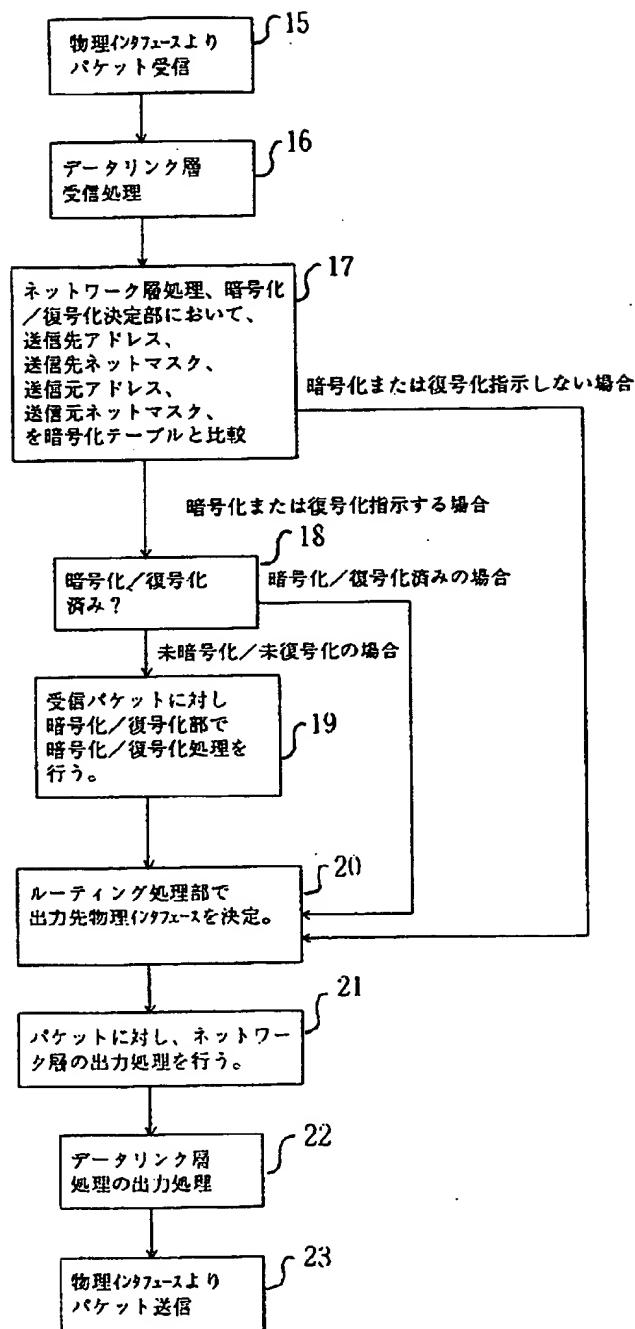
【図5】



【図6】

送信先アドレス	送信先ネットワークマスク	送信元アドレス	送信元ネットワークマスク	暗号化復号化種別
ネットワークD	ネットワークDのネットマスク	ネットワークA	ネットワークAのネットマスク	暗号化
ネットワークA	ネットワークAのネットマスク	ネットワークD	ネットワークDのネットマスク	復号化

【図4】



【図 7】

33
5

送信先アドレス	送信先ネットワークマスク	送信元アドレス	送信元ネットワークマスク	暗号化復号化種別
ネットワーク D	ネットワーク D のネットマスク	ネットワーク A	ネットワーク A のネットマスク	復号化
ネットワーク A	ネットワーク A のネットマスク	ネットワーク D	ネットワーク D のネットマスク	暗号化